

Prova Automática de Teoremas para Lógicas Modais

Cláudia Nalon

<http://www.cic.unb.br/~nalon>

nalon@cic.unb.br, nalon@unb.br

Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Motivação – I

● Provas em Sistemas Modais

Motivação

● Motivação – I

● Motivação – II

Overview

Lógica Proposicional

Lógica de Conhecimento

Conclusões

- Linguagens lógicas estão intrinsicamente ligadas ao conceito de computação (e.g. circuitos implementando um computador digital podem ser descritos através de linguagem proposicional).
- A utilização de linguagens lógicas para descrever problemas computacionais data da época em que os primeiros computadores digitais foram construídos.
- Datam da mesma época também, os esforços para se implementar provadores automáticos de teoremas.

Motivação – II

● Provas em Sistemas Modais

Motivação

● Motivação – I

● Motivação – II

Overview

Lógica Proposicional

Lógica de Conhecimento

Conclusões

- Desenvolvimentos teóricos, datando desta mesma época, fizeram com que as linguagens modais deixassem o contexto da discussão filosófica e fossem adotadas na descrição de problemas matemáticos e computacionais.
- Linguagens modais expressam tais problemas de modo natural, através, por exemplo, do uso das noções de necessidade, conhecimento, crença e tempo.
- Linguagens modais possuem **boas** características, ou seja, os problemas de decisão relativos a tais linguagens são computacionalmente tratáveis.

Roteiro

● Provas em Sistemas Modais

Motivação

Overview

● Roteiro

Lógica Proposicional

Lógica de Conhecimento

Conclusões

1. Lógica Proposicional:

notação, sintaxe, semântica, método de prova, renomeação;

2. Lógicas Epistêmicas:

motivação, sintaxe, semântica, resolução, exemplos.

Introdução e Sintaxe

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

● **Introdução e Sintaxe**

● Semântica

● Propriedades Semânticas

● Métodos de Prova – I

● Semântica e Prova

● Resolução

● CNF

● Exemplo I

● Eficiência

● Exemplo II

● Eficiência II

● Renomeação

● Exemplo II

● Eficiência II

● Exemplo

Lógica de Conhecimento

Conclusões

■ Sentenças complexas são construídas a partir destes símbolos e de conectivos:

◆ *Símbolos Proposicionais*: $\mathcal{P} = \{p, q, r, p', q', r', \dots\}$;

◆ *Constantes*: true, false;

◆ *Operadores Clássicos*:

$\neg\varphi$	(negação),
$(\varphi \wedge \phi)$	(conjunção),
$(\varphi \vee \phi)$	(disjunção),
$(\varphi \Rightarrow \phi)$	(implicação),
$(\varphi \Leftrightarrow \phi)$	(dupla implicação).

Semântica

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

● Introdução e Sintaxe

● Semântica

● Propriedades Semânticas

● Métodos de Prova – I

● Semântica e Prova

● Resolução

● CNF

● Exemplo I

● Eficiência

● Exemplo II

● Eficiência II

● Renomeação

● Exemplo II

● Eficiência II

● Exemplo

Lógica de Conhecimento

Conclusões

- Uma **valoração** é uma função π_0 a qual atribui um *valor de verdade* a cada um dos símbolos proposicionais:

$$\pi_0 : \mathcal{P} \rightarrow \{true, false\}$$

- A função de valoração é estendida para lidar com fórmulas complexas, e.g.:

$$\pi(\neg\varphi) = true \text{ se, e somente se, } \pi_0(\varphi) = false$$

$$\pi(\varphi \wedge \psi) = true \text{ se, e somente se, } \pi_0(\varphi) = true \text{ e } \pi_0(\psi) = true$$

Propriedades Semânticas

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

● Introdução e Sintaxe

● Semântica

● **Propriedades Semânticas**

● Métodos de Prova – I

● Semântica e Prova

● Resolução

● CNF

● Exemplo I

● Eficiência

● Exemplo II

● Eficiência II

● Renomeação

● Exemplo II

● Eficiência II

● Exemplo

Lógica de Conhecimento

Conclusões

- Uma valoração π **satisfaz** uma fórmula φ se, e somente se, $\pi(\varphi) = \text{true}$.
- Uma fórmula φ é **válida** se, e somente se, $\pi(\varphi) = \text{true}$ para toda valoração π .
- Uma fórmula φ é uma **contradição** se, e somente se, $\pi(\varphi) = \text{false}$ para toda valoração π .
- $\Gamma \models \varphi$: φ é consequência lógica de Γ .
 $\models \varphi$ abrevia $\emptyset \models \varphi$: φ é válida.

Métodos de Prova – I

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

- Um **cálculo** para uma determinada linguagem lógica consiste de um conjunto de **axiomas** e um conjunto de **regras de inferência**.
- A **prova de φ a partir de um conjunto de fórmulas Γ** é uma seqüência de fórmulas $\varphi_0, \dots, \varphi_n$, onde $\varphi_n = \varphi$ e cada φ_i é
 - ◆ um axioma;
 - ◆ um membro de Γ ; ou
 - ◆ foi obtido a partir da aplicação das regras de inferência às fórmulas anteriores na seqüência.
- $\Gamma \vdash \varphi$: existe uma prova de φ a partir de Γ ;
 $\vdash \varphi$ abrevia $\emptyset \vdash \varphi$: φ é um **teorema**.

Relação entre Semântica e Prova

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova

- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

- O cálculo é **consistente** se todo teorema é uma fórmula válida.

$$\vdash \varphi \implies \models \varphi$$

- O cálculo é **completo** se toda fórmula válida é um teorema.

$$\models \varphi \implies \vdash \varphi$$

- Uma lógica é **decidível** se existe um *procedimento*, cuja *terminação* seja garantida, que *determine* se uma dada fórmula é um teorema ou não.

Resolução

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova

● Resolução

- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$\text{[MRES1]} \quad \frac{(D \vee m_i) \quad (D' \vee \neg m_i)}{(D \vee D')}$$

- Fórmulas são primeiramente transformadas em sua *forma normal*.

$$(l_1 \vee \dots \vee l_n) \wedge (l_{n+1} \vee \dots \vee l_m) \wedge \dots \wedge (l_r \vee \dots \vee l_s)$$

- **Literal:** p ou $\neg p$, onde p é um símbolo proposicional.
- Disjunções de literais são chamadas de **cláusulas**.

Forma Normal Conjuntiva

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- **CNF**
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

1. implicações e duplas implicações são reescritos:

$$\varphi \Rightarrow \psi \longrightarrow (\neg\varphi \vee \psi)$$

$$\varphi \Leftrightarrow \psi \longrightarrow (\neg\varphi \vee \psi) \wedge (\varphi \vee \neg\psi)$$

2. negações são reescritas (De Morgan's):

$$\neg(\varphi \wedge \psi) \longrightarrow (\neg\varphi \vee \neg\psi)$$

$$\neg(\varphi \vee \psi) \longrightarrow (\neg\varphi \wedge \neg\psi)$$

3. duplas negações são eliminadas, i.e. $\neg\neg\varphi \longrightarrow \varphi$

4. leis distributivas são aplicadas:

$$\varphi \vee (\psi \wedge \chi) \longrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \chi)$$

$$\varphi \wedge (\psi \vee \chi) \longrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$$

Exemplo I

- Provas em Sistemas Modais

- Motivação

- Overview

- Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF

- Exemplo I

- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

- Lógica de Conhecimento

- Conclusões

$$(p \Leftrightarrow q) \vee (r \Leftrightarrow s)$$

1. $(p \Rightarrow q) \wedge (q \Rightarrow p) \vee ((r \Rightarrow s) \wedge (s \Rightarrow r))$

Exemplo I

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF

● Exemplo I

- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(p \Leftrightarrow q) \vee (r \Leftrightarrow s)$$

1. $((p \Rightarrow q) \wedge (q \Rightarrow p)) \vee ((r \Rightarrow s) \wedge (s \Rightarrow r))$
2. $((\neg p \vee q) \wedge (\neg q \vee p)) \vee ((\neg r \vee s) \wedge (\neg s \vee r))$

Exemplo I

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF

● Exemplo I

- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(p \Leftrightarrow q) \vee (r \Leftrightarrow s)$$

1. $((p \Rightarrow q) \wedge (q \Rightarrow p)) \vee ((r \Rightarrow s) \wedge (s \Rightarrow r))$
2. $((\neg p \vee q) \wedge (\neg q \vee p)) \vee ((\neg r \vee s) \wedge (\neg s \vee r))$
3. $((\neg p \vee q) \vee (\neg r \vee s)) \wedge ((\neg p \vee q) \vee (\neg s \vee r)) \wedge ((\neg q \vee p) \vee (\neg r \vee s)) \wedge ((\neg q \vee p) \vee (\neg s \vee r))$

Exemplo I

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF

● Exemplo I

- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(p \Leftrightarrow q) \vee (r \Leftrightarrow s)$$

1. $((p \Rightarrow q) \wedge (q \Rightarrow p)) \vee ((r \Rightarrow s) \wedge (s \Rightarrow r))$
2. $((\neg p \vee q) \wedge (\neg q \vee p)) \vee ((\neg r \vee s) \wedge (\neg s \vee r))$
3. $((\neg p \vee q) \vee (\neg r \vee s)) \wedge ((\neg p \vee q) \vee (\neg s \vee r)) \wedge ((\neg q \vee p) \vee (\neg r \vee s)) \wedge ((\neg q \vee p) \vee (\neg s \vee r))$

$$\begin{aligned} & ((\neg p \vee q \vee \neg r \vee s) \wedge \\ & (\neg p \vee q \vee r \vee \neg s) \wedge \\ & (p \vee \neg q \vee \neg r \vee s) \wedge \\ & (p \vee \neg q \vee r \vee \neg s)) \end{aligned}$$

Eficiência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$\begin{array}{l} (\neg R \vee R \vee \neg P \vee P) \wedge (\neg S \vee R \vee \neg P \vee P) \wedge \\ (\neg R \vee S \vee \neg P \vee P) \wedge (\neg S \vee S \vee \neg P \vee P) \wedge \\ (\neg R \vee R \vee \neg Q \vee P) \wedge (\neg S \vee R \vee \neg Q \vee P) \wedge \\ (\neg R \vee S \vee \neg Q \vee P) \wedge (\neg S \vee S \vee \neg Q \vee P) \wedge \\ (\neg R \vee R \vee \neg P \vee Q) \wedge (\neg S \vee R \vee \neg P \vee Q) \wedge \\ (\neg R \vee S \vee \neg P \vee Q) \wedge (\neg S \vee S \vee \neg P \vee Q) \wedge \\ (\neg R \vee R \vee \neg Q \vee Q) \wedge (\neg S \vee R \vee \neg Q \vee Q) \wedge \\ (\neg R \vee S \vee \neg Q \vee Q) \wedge (\neg S \vee S \vee \neg Q \vee Q) \end{array}$$

Eficiência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$\begin{array}{l} (\neg R \vee R \vee \neg P \vee P) \wedge (\neg S \vee R \vee \neg P \vee P) \wedge \\ (\neg R \vee S \vee \neg P \vee P) \wedge (\neg S \vee S \vee \neg P \vee P) \wedge \\ (\neg R \vee R \vee \neg Q \vee P) \wedge (\neg S \vee R \vee \neg Q \vee P) \wedge \\ (\neg R \vee S \vee \neg Q \vee P) \wedge (\neg S \vee S \vee \neg Q \vee P) \wedge \\ (\neg R \vee R \vee \neg P \vee Q) \wedge (\neg S \vee R \vee \neg P \vee Q) \wedge \\ (\neg R \vee S \vee \neg P \vee Q) \wedge (\neg S \vee S \vee \neg P \vee Q) \wedge \\ (\neg R \vee R \vee \neg Q \vee Q) \wedge (\neg S \vee R \vee \neg Q \vee Q) \wedge \\ (\neg R \vee S \vee \neg Q \vee Q) \wedge (\neg S \vee S \vee \neg Q \vee Q) \end{array}$$

Exemplo II

- Provas em Sistemas Modais

- Motivação

- Overview

- Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

- Lógica de Conhecimento

- Conclusões

$$(a \wedge b) \vee (c \wedge d)$$

$$\Rightarrow ((a \vee c) \wedge (a \vee d) \wedge (b \vee c) \wedge (b \vee d))$$

Exemplo II

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(a \wedge b) \vee (c \wedge d)$$

$$\Rightarrow ((a \vee c) \wedge (a \vee d) \wedge (b \vee c) \wedge (b \vee d))$$

$$(a \wedge b) \vee (c \wedge d \wedge e)$$

$$\Rightarrow ((a \vee c) \wedge (a \vee d) \wedge (a \vee e) \wedge (b \vee c) \wedge (b \vee d) \wedge (b \vee e))$$

Exemplo II

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(a \wedge b) \vee (c \wedge d)$$

$$\Rightarrow ((a \vee c) \wedge (a \vee d) \wedge (b \vee c) \wedge (b \vee d))$$

$$(a \wedge b) \vee (c \wedge d \wedge e)$$

$$\Rightarrow ((a \vee c) \wedge (a \vee d) \wedge (a \vee e) \wedge (b \vee c) \wedge (b \vee d) \wedge (b \vee e))$$

$$(a \wedge b \wedge f) \vee (c \wedge d \wedge e)$$

$$\Rightarrow ((a \vee c) \wedge (a \vee d) \wedge (a \vee e) \wedge (b \vee c) \wedge (b \vee d) \wedge (b \vee e) \wedge (f \vee c) \wedge (f \vee d) \wedge (f \vee e))$$

Eficiência II

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

■ Explosão combinatorial:

$$(l_1 \wedge \dots \wedge l_m) \vee (k_1 \wedge \dots \wedge k_n) \Rightarrow O(m \times n)$$

■ Em geral:

ψ	$p(\psi)$	$\bar{p}(\psi)$
$\varphi_1 \wedge \dots \wedge \varphi_n$	$\sum_{i=1}^n p(\varphi_i)$	$\prod_{i=1}^n \bar{p}(\varphi_i)$
$\varphi_1 \vee \dots \vee \varphi_n$	$\prod_{i=1}^n p(\varphi_i)$	$\sum_{i=1}^n \bar{p}(\varphi_i)$
$\varphi_1 \Rightarrow \varphi_2$	$\bar{p}(\varphi_1)p(\varphi_2)$	$p(\varphi_1) + \bar{p}(\varphi_2)$
$\varphi_1 \Leftrightarrow \varphi_2$	$p(\varphi_1)\bar{p}(\varphi_2) + \bar{p}(\varphi_1)p(\varphi_2)$	$p(\varphi_1)p(\varphi_2) + \bar{p}(\varphi_1)\bar{p}(\varphi_2)$
$\neg\varphi$	$\bar{p}(\varphi)$	$p(\varphi)$
atômico	1	1

Renomeação

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

- Técnica baseada na introdução de novos literais;
- Literais substituem subfórmulas;
- Introduce também cláusulas que dão significado a estes novos literais, dependendo da polaridade:

Seja φ a fórmula a ser substituída, então:

$$Pol(\varphi) > 0 \Rightarrow new_{\varphi} \Rightarrow \varphi$$

$$Pol(\varphi) < 0 \Rightarrow \varphi \Rightarrow new_{\varphi}$$

$$Pol(\varphi) = 0 \Rightarrow new_{\varphi} \Leftrightarrow \varphi$$

Exemplo II

- Provas em Sistemas Modais

- Motivação

- Overview

- Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

- Lógica de Conhecimento

- Conclusões

$$(a \wedge b \wedge f) \vee (c \wedge d \wedge e)$$

Exemplo II

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(a \wedge b \wedge f) \vee (c \wedge d \wedge e)$$

$$new_{(a \wedge b \wedge f)} \vee new_{(c \wedge d \wedge e)}$$

$$new_{(a \wedge b \wedge f)} \Rightarrow (a \wedge b \wedge f) \quad new_{(c \wedge d \wedge e)} \Rightarrow (c \wedge d \wedge e)$$

Exemplo II

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$(a \wedge b \wedge f) \vee (c \wedge d \wedge e)$$

$$new_{(a \wedge b \wedge f)} \vee new_{(c \wedge d \wedge e)}$$

$$new_{(a \wedge b \wedge f)} \Rightarrow (a \wedge b \wedge f) \quad new_{(c \wedge d \wedge e)} \Rightarrow (c \wedge d \wedge e)$$

$$\neg new_{(a \wedge b \wedge f)} \vee a$$

$$\neg new_{(c \wedge d \wedge e)} \vee c$$

$$\neg new_{(a \wedge b \wedge f)} \vee b$$

$$\neg new_{(c \wedge d \wedge e)} \vee d$$

$$\neg new_{(a \wedge b \wedge f)} \vee f$$

$$\neg new_{(c \wedge d \wedge e)} \vee e$$

Eficiência II

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

- Renomeação **pode** evitar explosão combinatorial:
 $O(m + n) \times O(m \times n)$;
- Pode-se computar, em tempo linear, se renomear uma subfórmula é mais vantajoso do que utilizar o procedimento padrão de transformação na forma clausal:

[Nonnengart at all, On Generating Small Clause Normal Forms]

- Esta verificação é feita através de um cálculo baseado em coeficientes, os quais determinam o quão frequentemente uma determinada subfórmula e sua negação serão duplicadas no decorrer da transformação padrão;
- A partir do cálculo destes coeficientes uma determinada inequação pode, então, ser resolvida e determinar se é melhor renomear ou não.

Exemplo

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

- Introdução e Sintaxe
- Semântica
- Propriedades Semânticas
- Métodos de Prova – I
- Semântica e Prova
- Resolução
- CNF
- Exemplo I
- Eficiência
- Exemplo II
- Eficiência II
- Renomeação
- Exemplo II
- Eficiência II
- Exemplo

Lógica de Conhecimento

Conclusões

$$\{p \Rightarrow q, q \Rightarrow r\} \vdash \{p \Rightarrow r\}$$

1. $\neg p \vee q$
2. $\neg q \vee r$
3. p
4. $\neg r$
5. $\neg q$ [4, 2, RES]
6. $\neg p$ [5, 1, RES]
7. **false** [6, 3, RES]

Introdução

- Provas em Sistemas Modais

- Motivação

- Overview

- Lógica Proposicional

- Lógica de Conhecimento

- **Introdução**

- Exemplo - Formalização

- Sintaxe

- Semântica

- Resolução

- Exemplo

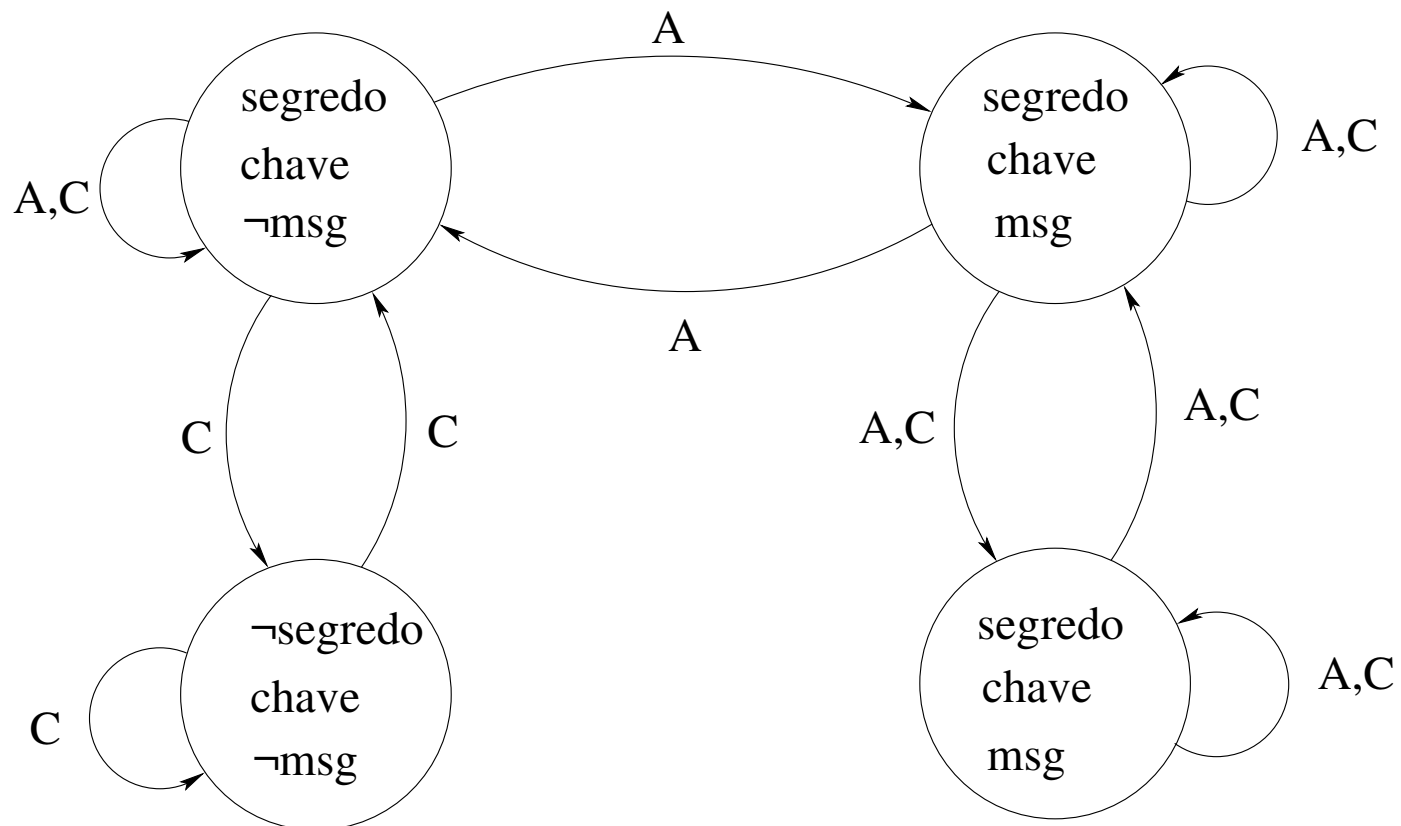
- Exemplo Acabado

- Regras de Inferência

- Exemplo

- Conclusões

- Úteis na especificação de sistemas multi-agentes, sistemas distribuídos, protocolos, bases de conhecimento, etc.



Exemplo - Formalização

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

● Introdução

● Exemplo - Formalização

● Sintaxe

● Semântica

● Resolução

● Exemplo

● Exemplo Acabado

● Regras de Inferência

● Exemplo

Conclusões

Introduz uma nova modalidade para cada agente: $K_i \varphi$.

K_{Alice} segredo

$K_{Alice} K_{Charlie}$ chave

$K_{Alice} K_{Charlie} (\text{chave} \wedge \text{send}(Alice, Charlie, msg) \Rightarrow K_{Charlie}$
segredo)

$\text{send}(Alice, Charlie, msg) \Rightarrow K_{Alice} K_{Charlie}$ segredo

$K_{Alice} K_{Bob} \neg \text{chave} \Rightarrow K_{Alice} K_{Bob} \neg$ segredo

Sintaxe

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

● Introdução

● Exemplo - Formalização

● Sintaxe

● Semântica

● Resolução

● Exemplo

● Exemplo Acabado

● Regras de Inferência

● Exemplo

Conclusões

Axiomatização: $KL_{(n)} = K, T, D, 4, 5$.

K:	$\vdash K_i (\varphi \Rightarrow \psi) \Rightarrow (K_i \varphi \Rightarrow K_i \psi)$
T:	$\vdash K_i \varphi \Rightarrow \varphi$
D:	$\vdash K_i \varphi \Rightarrow \neg K_i \neg \varphi$
4:	$\vdash K_i \varphi \Rightarrow K_i K_i \varphi$
5:	$\vdash \neg K_i \neg \varphi \Rightarrow K_i \neg K_i \neg \varphi$

Sintaxe:

- *Símbolos Proposicionais*: $\mathcal{P} = \{p, q, r, p', q', r', \dots\}$;
- *Constantes*: true, false;
- *Operadores Clássicos*: $\neg\varphi$, $(\varphi \wedge \phi)$, $(\varphi \vee \phi)$, $(\varphi \Rightarrow \phi)$, $(\varphi \Leftrightarrow \phi)$;
- *Operadores Modais*: $K_i \varphi$, $\forall i \in \mathcal{A}$, where $\mathcal{A} = \{1, \dots, n\}$.

Semântica

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe

● Semântica

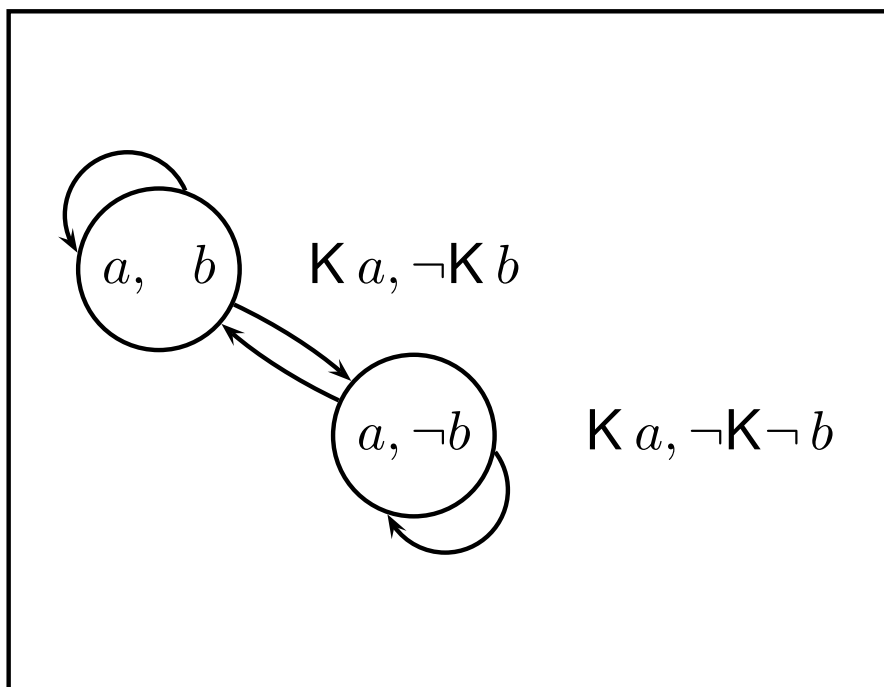
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

Semântica baseada em estruturas de Kripke

$$M = \langle W, \mathcal{K}_1, \dots, \mathcal{K}_n, \pi \rangle$$

onde W é um conjunto de mundos; \mathcal{K}_i são relações de equivalência; e $\pi : W \times \mathcal{P} \rightarrow \{true, false\}$ é uma função.



Resolução

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

Cláusulas na forma: $\square^* \bigwedge A = \bigwedge \square^* A$

Inicial

$$\text{start} \Rightarrow \bigvee_{b=1}^r l_b$$

K_i

$$\text{true} \Rightarrow \bigvee_{b=1}^r m_{ib}$$

Literais

$$\text{true} \Rightarrow \bigvee_{b=1}^r l_b$$

Exemplo

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

Exemplo

- Provas em Sistemas Modais

- Motivação

- Overview

- Lógica Proposicional

- Lógica de Conhecimento

- Introdução

- Exemplo - Formalização

- Sintaxe

- Semântica

- Resolução

- Exemplo

- Exemplo Acabado

- Regras de Inferência

- Exemplo

- Conclusões

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

1. **start** $\Rightarrow t_1$

2. $t_1 \Rightarrow \neg K_1 K_2 (a \Rightarrow b) \vee K_1 (K_2 a \Rightarrow K_2 b)$

Exemplo

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

1. **start** $\Rightarrow t_1$
2. $t_1 \Rightarrow \neg K_1 K_2 (a \Rightarrow b) \vee K_1 (K_2 a \Rightarrow K_2 b)$
3. $t_1 \Rightarrow \neg K_1 \neg t_2 \vee K_1 t_3$
4. $t_2 \Rightarrow \neg K_2 (a \Rightarrow b)$
5. $t_3 \Rightarrow (K_2 a \Rightarrow K_2 b)$

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

Exemplo

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

1. **start** $\Rightarrow t_1$
2. $t_1 \Rightarrow \neg K_1 K_2 (a \Rightarrow b) \vee K_1 (K_2 a \Rightarrow K_2 b)$
3. $t_1 \Rightarrow \neg K_1 \neg t_2 \vee K_1 t_3$
4. $t_2 \Rightarrow \neg K_2 (a \Rightarrow b)$
5. $t_3 \Rightarrow (K_2 a \Rightarrow K_2 b)$
6. $\neg t_1 \vee \neg K_1 \neg t_2 \vee K_1 t_3$
7. $t_2 \Rightarrow \neg K_2 \neg t_4$
8. $t_4 \Rightarrow \neg(a \Rightarrow b)$

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

Exemplo

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

1. **start** $\Rightarrow t_1$
2. $t_1 \Rightarrow \neg K_1 K_2 (a \Rightarrow b) \vee K_1 (K_2 a \Rightarrow K_2 b)$
3. $t_1 \Rightarrow \neg K_1 \neg t_2 \vee K_1 t_3$
4. $t_2 \Rightarrow \neg K_2 (a \Rightarrow b)$
5. $t_3 \Rightarrow (K_2 a \Rightarrow K_2 b)$
6. $\neg t_1 \vee \neg K_1 \neg t_2 \vee K_1 t_3$
7. $t_2 \Rightarrow \neg K_2 \neg t_4$
8. $t_4 \Rightarrow \neg(a \Rightarrow b)$
9. $\neg t_2 \vee \neg K_2 \neg t_4$
10. $\neg t_4 \vee a$
11. $\neg t_4 \vee \neg b$

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

Exemplo

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

1. **start** $\Rightarrow t_1$
2. $t_1 \Rightarrow \neg K_1 K_2 (a \Rightarrow b) \vee K_1 (K_2 a \Rightarrow K_2 b)$
3. $t_1 \Rightarrow \neg K_1 \neg t_2 \vee K_1 t_3$
4. $t_2 \Rightarrow \neg K_2 (a \Rightarrow b)$
5. $t_3 \Rightarrow (K_2 a \Rightarrow K_2 b)$
6. $\neg t_1 \vee \neg K_1 \neg t_2 \vee K_1 t_3$
7. $t_2 \Rightarrow \neg K_2 \neg t_4$
8. $t_4 \Rightarrow \neg(a \Rightarrow b)$
9. $\neg t_2 \vee \neg K_2 \neg t_4$
10. $\neg t_4 \vee a$
11. $\neg t_4 \vee \neg b$
12. $\neg t_3 \Rightarrow \neg K_2 a \vee K_2 b$

Exemplo Acabado

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

$$K_1 K_2 (a \Rightarrow b) \Rightarrow K_1 (K_2 a \Rightarrow K_2 b)$$

1. **start** $\Rightarrow t_1$
2. **true** $\Rightarrow \neg t_1 \vee \neg K_1 \neg t_2 \vee K_1 t_3$
3. **true** $\Rightarrow \neg t_2 \vee \neg K_2 \neg t_4$
4. **true** $\Rightarrow \neg t_4 \vee a$
5. **true** $\Rightarrow \neg t_4 \vee \neg b$
6. **true** $\Rightarrow \neg t_3 \vee \neg K_2 a \vee K_2 b$

Regras de Inferência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

$$\begin{array}{l} \text{[MRES1]} \quad \text{true} \Rightarrow (D \vee m_i) \\ \text{true} \Rightarrow (D' \vee \neg m_i) \\ \hline \text{true} \Rightarrow (D \vee D') \end{array}$$

Exemplos

$$1. \quad \text{true} \Rightarrow \neg x \vee y$$

$$2. \quad \text{true} \Rightarrow \neg z \vee \neg y$$

$$3. \quad \text{true} \Rightarrow \neg x \vee \neg z \quad [1,2,M1]$$

$$1. \quad \text{true} \Rightarrow \neg x \vee K_1 y$$

$$2. \quad \text{true} \Rightarrow \neg z \vee \neg K_1 y$$

$$3. \quad \text{true} \Rightarrow \neg x \vee z \quad [1,2,M1]$$

$$1. \quad \text{true} \Rightarrow \neg x \vee K_1 y$$

$$2. \quad \text{true} \Rightarrow \neg z \vee \neg K_2 y$$

$$3. \quad \text{true} \Rightarrow \neg w \vee \neg y \vee \neg K_2 z$$

Regras de Inferência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

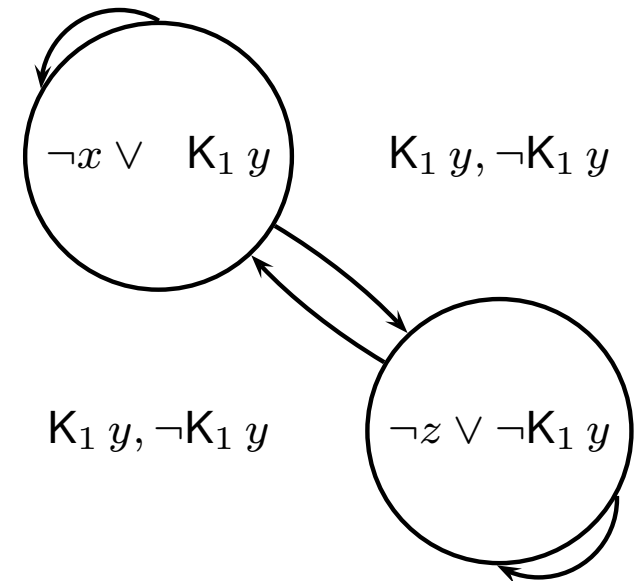
- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

$$\begin{array}{l} \text{[MRES2]} \quad \text{true} \Rightarrow (D \vee K_i l) \\ \text{true} \Rightarrow (D' \vee K_i \neg l) \\ \hline \text{true} \Rightarrow (D \vee D') \end{array}$$

Exemplo

1. $\text{true} \Rightarrow \neg x \vee K_1 y$
2. $\text{true} \Rightarrow \neg z \vee \neg K_1 y$
3. $\text{true} \Rightarrow \neg x \vee z$ [1,2,M2]



Regras de Inferência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

● Introdução

● Exemplo - Formalização

● Sintaxe

● Semântica

● Resolução

● Exemplo

● Exemplo Acabado

● Regras de Inferência

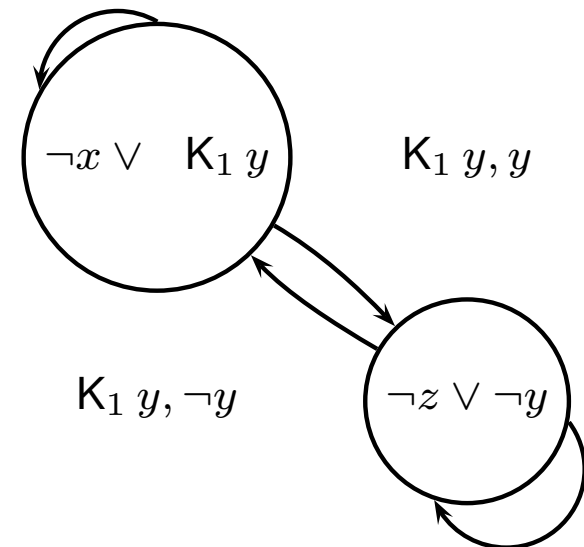
● Exemplo

Conclusões

$$\begin{array}{l}
 \text{[MRES3]} \quad \text{true} \Rightarrow (D \vee K_i l) \\
 \text{true} \Rightarrow (D' \vee \neg l) \\
 \hline
 \text{true} \Rightarrow (D \vee D')
 \end{array}$$

Exemplo

$$\begin{array}{l}
 1. \quad \text{true} \Rightarrow \neg x \vee K_1 y \\
 2. \quad \text{true} \Rightarrow \neg z \vee \neg y \\
 \hline
 3. \quad \text{true} \Rightarrow \neg x \vee z \quad [1,2,M3]
 \end{array}$$



Regras de Inferência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

$$\begin{array}{l} \text{[MRES4]} \quad \boxed{}^* (\mathbf{true} \Rightarrow (D \vee \neg K_i l)) \\ \boxed{}^* (\mathbf{true} \Rightarrow (D' \vee l)) \\ \hline \boxed{}^* (\mathbf{true} \Rightarrow (D \vee \neg K_i \neg D')) \end{array}$$

Justificativa

1. $\boxed{}^* (\mathbf{true} \Rightarrow (D' \vee l))$
2. $\boxed{}^* (\neg D' \Rightarrow l)$
3. $\boxed{}^* K_i (\neg D' \Rightarrow l)$
4. $\boxed{}^* (K_i \neg D' \Rightarrow K_i l)$
5. $\boxed{}^* (\mathbf{true} \Rightarrow (\neg K_i \neg D' \vee K_i l))$

Exemplo

1. $\mathbf{true} \Rightarrow \neg x \vee \neg K_1 y$
2. $\mathbf{true} \Rightarrow \neg z \vee \neg y$
3. $\mathbf{true} \Rightarrow \neg x \vee \neg K_1 z$ [1,2,M4]

Regras de Inferência

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência
- Exemplo

Conclusões

$$\text{[MRES5]} \quad \frac{\text{true} \Rightarrow (L \vee K_i l_1 \vee K_i l_2 \vee \dots)}{\text{true} \Rightarrow (L \vee l_1 \vee l_2 \vee \dots)}$$

Exemplos

$$\begin{array}{l} 1. \quad \text{true} \Rightarrow \neg x \vee K_1 y \\ \hline 2. \quad \text{true} \Rightarrow \neg x \vee y \quad [1, M5] \end{array}$$

$$1. \quad \frac{\text{true} \Rightarrow \neg x \vee K_1 y \vee \neg K_1 z}{\text{true} \Rightarrow \neg x \vee K_1 y \vee \neg K_1 z}$$

$$\begin{array}{l} 1. \quad \text{true} \Rightarrow \neg x \vee K_1 y \\ 2. \quad \text{true} \Rightarrow \neg z \vee K_2 \neg y \\ 3. \quad \text{true} \Rightarrow \neg w \vee \neg y \vee \neg K_2 z \\ \hline 4. \quad \text{true} \Rightarrow \neg x \vee y \quad [1, M5] \\ 5. \quad \text{true} \Rightarrow \neg x \vee \neg z \quad [4, 2, M3] \\ 6. \quad \text{true} \Rightarrow \neg x \vee \neg w \vee \neg K_2 z \quad [3, 4, M3] \end{array}$$

Exemplo

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

- Introdução
- Exemplo - Formalização
- Sintaxe
- Semântica
- Resolução
- Exemplo
- Exemplo Acabado
- Regras de Inferência

● Exemplo

Conclusões

$$K_1 K_2 (a \Rightarrow b) \Rightarrow (K_1 K_2 a \Rightarrow K_1 K_2 b)$$

- | | | | | | |
|-----|--------------|---------------|--|-------------|--|
| 1. | start | \Rightarrow | x | | |
| 2. | true | \Rightarrow | $\neg x \vee K_1 y$ | | |
| 3. | true | \Rightarrow | $\neg y \vee K_2 z$ | | |
| 4. | true | \Rightarrow | $\neg z \vee \neg a \vee b$ | | |
| 5. | true | \Rightarrow | $\neg x \vee K_1 t$ | | |
| 6. | true | \Rightarrow | $\neg t \vee K_2 a$ | | |
| 7. | true | \Rightarrow | $\neg x \vee \neg K_1 \neg r$ | | |
| 8. | true | \Rightarrow | $\neg r \vee \neg K_2 b$ | | |
| 9. | true | \Rightarrow | $\neg r \vee \neg K_2 z \vee \neg K_2 a$ | [8, 4, M4] | |
| 10. | true | \Rightarrow | $\neg r \vee \neg K_2 z \vee \neg t$ | [9, 6, M1] | |
| 11. | true | \Rightarrow | $\neg r \vee \neg y \vee \neg t$ | [10, 3, M1] | |
| 12. | true | \Rightarrow | $\neg x \vee \neg K_1 y \vee \neg K_1 t$ | [11, 7, M4] | |
| 13. | true | \Rightarrow | $\neg x \vee \neg K_1 y$ | [12, 5, M1] | |
| 14. | true | \Rightarrow | $\neg x$ | [13, 2, M1] | |
| 15. | start | \Rightarrow | false | [14, 1, l1] | |

Resultados

● Provas em Sistemas Modais

Motivação

Overview

Lógica Proposicional

Lógica de Conhecimento

Conclusões

● Resultados

- Terminação, Consistência e Completude;
- Facilmente combinado com resolução temporal
- Lógicas que admitem interações:

$$\bigcirc K_i \varphi \Rightarrow K_i \bigcirc \varphi$$

- Resolução para outras lógicas modais:
 1. Como obter formas normais que sejam melhores;
 2. Método de prova baseado em resolução levando-se em consideração a teoria da correspondência;
 3. Produção de modelos a partir de fórmulas que não sejam válidas.